

EXHIBIT A

FEDERAL PUBLIC DEFENDER
CENTRAL DISTRICT OF CALIFORNIA
321 EAST 2nd STREET
LOS ANGELES, CALIFORNIA 90012-4202
213-894-2854
213-894-0081 FAX

CUAUHTEMOC ORTEGA
Federal Public Defender
AMY M. KARLIN
Chief Deputy

ANGELA VIRAMONTES
Riverside Branch Chief
KELLEY MUNOZ
Santa Ana Branch Chief
K. ELIZABETH DAHLSTROM
Chief, Capital Habeas Unit

Direct Dial: (213) 894-4795

March 5, 2023

Mark Williams
Matt O'Brien
Brian Faerstein
Assistant United States Attorneys
United States Attorney's Office
312 N. Spring Street
Los Angeles, CA 90012

Re: Third Supplemental Discovery Request
United States v. Jerry Boylan, 2:20-CR-00600-GW

Dear Mr. Williams, Mr. O'Brien, and Mr. Faerstein:

We are writing to memorialize prior discovery requests and reiterate our prior request for discovery pertaining to the digital devices in the government's possession.

On August 10, 2022, we requested complete extractions of all electronic devices searched by the government. *See* Second Supplemental Discovery Requested (dated August 10, 2022). By email you indicated that you would only be providing limited portions of the data from the devices; specifically, the data that was bookmarked by the agent during his review of the complete contents of the devices. You requested that we provide authority for producing the complete image of any device not belonging to Mr. Boylan. I replied and directed you to Federal Rule of Criminal Procedure 16(a)(1)(E). I also informed you of your office's practice of producing the complete contents of cell phones belonging to decedents in drug overdose cases and directed to you one example of a case where your office produced a decedent's cell phone as a matter of course.

//

March 5, 2023

Page 2

Rule 16(a)(1)(E) provides:

(E) Documents and Objects. Upon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and:

- (i) the item is material to preparing the defense;
- (ii) the government intends to use the item in its case-in-chief at trial; or
- (iii) the item was obtained from or belongs to the defendant.

The complete contents of the devices must be produced under prongs (i) and (ii). The devices have data that the government intends to introduce in its case-in-chief. Because you intend to use the device and data recovered from it at trial, you must produce the device for inspection and copying by the defense under the plain terms of Rule 16(a)(1)(E)(ii). Because the government intends to use items obtained from the devices to prove Mr. Boylan's guilt, the analysis of the devices is also material to preparing a defense and must be produced under Rule 16(a)(1)(E)(i).

Without the complete image, the defense is unable to: (1) authenticate/validate the evidence being produced; (2) analyze the seized item properly for defense strategy purposes; (3) determine how an artifact was utilized by the user;¹ (4) verify the findings of potential government witnesses regarding electronically stored information; and (5) verify or dispute the veracity of claims by witnesses pertaining to the digital evidence.

What can be uncovered during a complete analysis of a forensic device is explained by Special Agent Jamie E. Wray in the declaration he submitted in support of search warrant #45A-LA-3161932 (BOYLAN_00271515). In Paragraph 34 he declares:

¹ Just as forensic pathologists can examine a cadaver's fractures, bruises, calluses, and scars to determine what happened to that body over a person's lifetime, so too can a computer forensic analyst examine a hard drive to learn how a computer was used. When a computer user accesses a web site, opens a file, launches a program, starts the computer, shuts it down, logs on, logs off, installs software, removes software, or attaches a flash drive, hard drives reflect those actions. Forensic analysts term such evidence "artifacts." Like archaeological artifacts showing how people once lived, forensic artifacts show how computers were used. Log files show what software programs did. Virtual memory paging files can reveal what was once in memory. Temporary files and link files can reveal that someone created, opened, or saved particular files. When a user saves a file in Microsoft Word, for example, eight different files or folders are created, modified, or accessed in sixteen different steps, all occurring in less than a second. In Windows, a vast configuration database, called the "registry," is an evidence treasure chest, showing recent user commands, recent files opened, recent network drives accessed, recent web sites visited, whether USB flash drives were attached, what Wi-Fi wireless access points have been used, and more. Goldfoot, J., *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 127 (2011)

March 5, 2023

Page 3

Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software."

//

//

//

//

//

//

March 5, 2023

Page 4

The defense must be permitted to conduct an analysis of the complete extraction for the same exact reasons cited by SA Wray. Because the agent who reviewed and bookmarked the extraction does not know the nature of the defense, the government cannot guarantee compliance with Rule 16 or *Brady* by the limited production from the devices. We are reiterating our request for the complete extraction of all devices in the government's possession—not just what the agent(s) decided to bookmark as relevant and produce as a reporting of their findings. We would greatly appreciate a response as soon as possible—ideally within the week, as we intend to litigate this issue as soon as possible to avoid any trial delays.

Sincerely,

/S/

Georgina Wakefield

Gabriela Rivera

Julia Deixler

EXHIBIT B



United States Department of Justice

United States Attorney's Office Central District of California

Mark A. Williams
Assistant United States Attorney
Environmental and Community Safety Crimes Section
Phone: (213) 894-3359
E-mail: mark.a.williams@usdoj.gov

1300 United States Courthouse
312 North Spring Street
Los Angeles, California 90012

March 9, 2023

VIA EMAIL

Georgina Wakefield
Gabriela Rivera
Julia Deixler
Deputy Federal Public Defenders
321 East 2nd Street
Los Angeles, California 90012

Re: United States v. Jerry Nehl Boylan,
CR No. 22-482-GW

Dear Counsel:

We are writing to respond to your letter dated March 5, 2023, concerning your request for discovery related to four digital devices. Our position has not changed since September 2022 when we last discussed this issue with you.

As we understand your position, in every case heading to trial where the government intends to rely on evidence seized from a third party's digital device pursuant to a search warrant, the defendant would be entitled to receive a complete mirrored copy of the digital device even though the search warrant authorized the government to seize only a limited set of responsive data from that device. If this were correct, the limitations imposed by federal courts pursuant to nearly every Rule 41 search warrant for a digital device would be rendered meaningless. Every defendant could simply argue that he or she is unable to authenticate/validate/verify the findings of the agent(s) who performed the search of the digital device without getting the complete extraction; the government would then be forced to produce information to which it has no legal right to access pursuant to the warrant; and the defense would obtain far more information from the digital device than the government possesses, leading to inevitable disputes about reciprocal discovery obligations. In our view, your position would turn the well-established process, and Rule 41 itself, on its head.

Similarly, for digital devices searched pursuant to a victim's family's consent, your position appears to be that the defense is entitled to search the entire device. This would cause several problems, including raising privacy concerns and dissuading victims or their families from consenting to a limited search in the first place.

Wakefield / Rivera / Deixler
Deputy Federal Public Defenders
RE: United States v. Jerry Boylan, CR No. 22-482-GW
March 9, 2023
Page 2

If we are misunderstanding your position, or if you have any judicial opinions backing your position, please let us know. Respectfully, we do not find persuasive your reliance on the plain language of Rule 16 and a single decision by one of our colleagues in a very different prosecution.

If you simply disagree with us, we respectfully request that you file a motion as soon as possible so that this issue can be litigated without delaying the trial. As you know, we communicated our position on this issue to you six months ago.

Please let us know if you have any questions or would like to further discuss any of the matters raised above.

Very truly yours,

/s/

MARK A. WILLIAMS
MATTHEW W. O'BRIEN
BRIAN R. FAERSTEIN
Assistant United States Attorneys

EXHIBIT C

UNITED STATES DISTRICT COURT

for the
Central District of California

In the Matter of the Search of
The Passenger Vessel Conception Wreckage

Case No. 2:19-MJ-03738

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment A-4

located in the Central District of California, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B-4

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
Title 18, United States Code, Section 1115

Offense Description
Misconduct or Neglect of Ship Officer Resulting
in Destruction of a Person

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (*give exact ending date if more than 30 days: _____*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: 9/7/19

City and state: Santa Barbara, CA

AUSA: Mark Williams x3359 & Joseph Johns x4536

Applicant's signature

CGIS Special Agent Jaime Wray

Printed name and title

Honorable Louise A. LaMothe

Judge's signature

Printed name and title

ATTACHMENT A-4

THE SUBJECT PREMISES

SUBJECT PREMISES A-4 is the vessel P/V CONCEPTION, Official Number 638133, including all remains of the wreckage, hull, and/or structures, and all debris and/or materials associated with the P/V CONCEPTION, including any digital devices recovered from the P/V CONCEPTION's wreckage and/or debris field (collectively, the "P/V CONCEPTION WRECKAGE"). The name "Conception" and the Official Number 638133 are painted on the side of the hull.

ATTACHMENT B-4

I. ITEMS TO BE SEIZED

The following is a list of items to be seized from SUBJECT PREMISES A-4, namely, the P/V CONCEPTION WRECKAGE, which constitute evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1115 (Seaman's Manslaughter):

1. The Passenger Vessel ("P/V") CONCEPTION, including all remains of the wreckage, hull, and/or structures, and all debris and/or materials associated with the P/V CONCEPTION, including any digital devices recovered from the P/V CONCEPTION's wreckage and/or debris field.

2. Evidence relating to the origin of the fire aboard the P/V CONCEPTION on or about September 2, 2019.

3. Evidence relating to the causation of the fire aboard the P/V CONCEPTION on or about September 2, 2019.

4. Evidence of custom, defective, and/or non-compliant electrical equipment, systems, and/or components on the P/V CONCEPTION.

5. Evidence of custom, defective, or non-compliant fire detection or suppression systems on the P/V CONCEPTION.

6. Evidence of custom, defective, and/or non-compliant passenger safety and/or evacuation structures, systems, and/or procedures on the P/V CONCEPTION.

7. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

8. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

g. applications, utility programs, compilers, interpreters, or other software, as well as documentation and

manuals, that may be necessary to access the device or to conduct a forensic examination of it;

h. records of or information about Internet Protocol addresses used by the device;

i. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

9. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

10. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to

store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

11. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and

attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques[, including to search for known images of child pornography].

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

12. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.

Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

13. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

- a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;
- b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;
- c. Any magnetic, electronic, or optical storage device capable of storing digital data;
- d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;
- e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;
- f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and
- g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

14. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, JAIME E. WRAY, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the United States Coast Guard Investigative ("CGIS"), and have been so employed since February 2018. Before that, from 2005 to 2017, I worked as a Boarding Officer conducting at sea and in port safety boarding and inspections of hundreds of vessels. I am a graduate of the Federal Law Enforcement Training Center Criminal Investigator Training Program. I am also a graduate of the U.S. Coast Guard ("USCG") Maritime Law Enforcement Academy. I have specialized training and experience in USCG Port State Control Vessel Inspections, including inspections of the vessel itself, safety equipment, engineering equipment, navigation equipment, and operations materials.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of search warrants for the following premises for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1115 (Seaman's Manslaughter):

a. The business premises operated by TRUTH AQUATICS, INC., and/or SEA LANDING, located at 301 West Cabrillo Boulevard, Santa Barbara, California, which is further described in Attachment A-1, for the items to be seized described in Attachment B-1 ("SUBJECT PREMISES A-1").

b. The Passenger Vessel ("P/V") TRUTH located at 301 West Cabrillo Boulevard, Santa Barbara, California, which is further described in Attachment A-2 for the items to be seized described in Attachment B-2 ("SUBJECT PREMISES A-2").

c. The P/V VISION located at 301 West Cabrillo Boulevard, Santa Barbara, California, which is further described in Attachment A-3, for the items to be seized described in Attachment B-3 ("SUBJECT PREMISES A-3").

d. The P/V CONCEPTION, including all remains of the wreckage, hull, and/or structures, and all debris and/or materials associated with the P/V CONCEPTION, including any digital devices recovered from the P/V CONCEPTION's wreckage and/or debris field (collectively, the "P/V CONCEPTION WRECKAGE"), which is further described in Attachment A-4, for the items to be seized described in Attachment B-4 ("SUBJECT PREMISES A-4").

3. Attachments A-1, A-2, A-3, A-4, B-1, B-2, B-3, and B-4 are incorporated herein by reference.

4. Due to the technical nature of marine industry terminology, engineering, and documentation it is the intention of law enforcement personnel to be assisted by subject matter specialists and/or experts during the execution of the search warrants as well as the duration of the searches, evidence review, and analysis.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and

witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. THE REGULATORY AND STATUTORY BACKGROUND

A. The United States Coast Guard Regulations Regarding Inspection and Certification of Small Passenger Vessels (Under 100 Gross Tons)

6. The United States Coast Guard regulates, inspects, and certifies the operation of small passenger vessels. These regulations are known as the "T-Boat" regulations, and are set forth in Title 46, Subchapter T, Part 175. 46 C.F.R. § 175.100.

7. The T-Boat regulations apply to the operation of all vessels of less than 100 gross tons that carry 150 or less passengers, or have overnight accommodations for 49 or less passengers, and (in relevant part) that:

a. Carry more than six passengers, including at least one for hire; or

b. Is chartered by the owner or the owner's representative and is carrying more than six passengers.

8. The T-Boat regulations mandate that the owner, charterer, master, or managing operator of a vessel carrying overnight passengers shall have a suitable number of watchmen patrol throughout the vessel during the nighttime, whether or not the vessel is underway, to guard against, and give alarm in

the case of, fire, man overboard, or other dangerous situation.

46 C.F.R. § 185.410.

B. The Seaman's Manslaughter Statute

9. Title 18, United States Code, Section 1115 criminalizes the misconduct or neglect of ship officers that result in the destruction of the life of any person. The statute specifically provides as follows:

Every captain, engineer, pilot, or other person employed on any steamboat or vessel, by whose misconduct, negligence, or inattention to his duties on such vessel the life of any person is destroyed, and every owner, charterer, inspector, or other public officer, through whose fraud, neglect, connivance, misconduct, or violation of law the life of any person is destroyed, shall be fined under this title or imprisoned not more than ten years, or both.

When the owner or charterer of any steamboat or vessel is a corporation, any executive officer of such corporation, for the time being actually charged with the control and management of the operation, equipment, or navigation of such steamboat or vessel, who has knowingly and willfully caused or allowed such fraud, neglect, connivance, misconduct, or violation of law, by which the life of any person is destroyed, shall be fined under this title or imprisoned for not more than ten years, or both.

IV. SUMMARY OF PROBABLE CAUSE

10. The P/V CONCEPTION, Official Number ("O.N.") 638133, was a 75-foot long passenger vessel owned by the FRITZLER FAMILY TRUST DTD 7/27/92 and operated by TRUTH AQUATICS, INC. The vessel was consumed by a fire in the early morning hours of September 2, 2019, killing 33 passengers and one crewmember. The vessel subsequently sank near Santa Cruz Island, California.

11. The applicable federal regulations required the owner, charterer, master, or managing operator of the vessel to have a suitable number of watchmen patrol throughout the vessel during the nighttime, whether or not the vessel was underway, to guard against, and give alarm in the case of fire or other dangerous situations.

12. Furthermore, the vessel was required by its Certificate of Inspection ("COI"), issued by the USCG, to conduct roving patrols when the passenger bunks were occupied. As discussed in more detail below, although passenger bunks were occupied by 33 passengers and one crewmember at the time of the fire on September 2, 2019, there was no roving patrol or crewmember standing watch at the time. Instead, every crewmember aboard the vessel was asleep. No passengers survived the fire.

V. STATEMENT OF PROBABLE CAUSE

A. Fire Aboard the P/V CONCEPTION

13. Based on my review of USCG materials and discussions with witnesses, first responders, and law enforcement agents, I learned the following information:

a. that at approximately 3:30 a.m. the USCG received a "may day" distress call over the radio. The USCG subsequently determined, based on additional radio calls and information, that the P/V CONCEPTION was on fire near Santa Cruz Island, California.

b. the P/V CONCEPTION was ultimately destroyed by the fire.

c. One crewmember and all 33 passengers aboard the vessel were killed as a result of the fire.

B. Lack of Watchstanding and Roving Patrols Aboard the P/V CONCEPTION

14. The P/V CONCEPTION had a COI that was valid from November 19, 2014, through November 19, 2019. The COI indicates that the vessel had a delivery date of July 1, 1981. The document also sets forth various requirements that the vessel must comply with. In the "Route Permitted And Conditions of Operation" section of the Certificate of Inspection, it states:

"A MEMBER OF THE VESSEL'S CREW SHALL BE DESIGNATED BY THE MASTER AS A ROVING PATROL AT ALL TIMES, WHETHER OR NOT THE VESSEL IS UNDERWAY, WHEN THE PASSENGER'S BUNKS ARE OCCUPIED."

15. I have reviewed written statements provided and signed by crewmember M.F., crewmember M.K., crewmember R.S., second captain C.M., and captain J.B. to USCG inspectors after the fire on or about September 2, 2019. All of the statements indicate that the crewmembers, second captain, and captain were woken by a fire aboard the P/V CONCEPTION early in the morning on September 2, 2019. Based on these written statements, I am informed and believe that all of these crewmembers were asleep when the fire at issue started and ultimately destroyed the P/V CONCEPTION.

16. USCG-CGIS and FBI special agents have listened to a recorded interview on September 4, 2019, with crewmember M.F. who was a deckhand aboard the P/V CONCEPTION at the time of the

fire. Based on my discussions with those agents, the crewmembers stated the following, among other things:

a. M.F. confirmed that there was no fire watch or anchor watch aboard the P/V CONCEPTION, and that those were not in their procedures.

17. On September 6, 2019, USCG-CGIS, FBI, and ATF special agents interviewed crewmember C.M., the second captain aboard the P/V CONCEPTION at the time the vessel caught fire. The interview was recorded. Based on my discussions with those agents, I learned that second captain C.M. stated the following, among other things:

a. The crew aboard the P/V CONCEPTION did not conduct roving patrols or have a crewmember standing watch at night, including when the fire occurred on September 2, 2019.

b. All crewmembers aboard the P/V CONCEPTION were sleeping at the time of the fire on September 2, 2019.

C. The P/V CONCEPTION WRECKAGE and Debris Field

18. Based upon my conversations with law enforcement officers and others engaged in the recovery of the P/V CONCEPTION WRECKAGE from the seabed, it is my understanding that there is a large debris field associated with the wreckage. The debris field contains all manner of evidence and material that was associated with the P/V CONCEPTION as it burned and sank. This evidence includes a number of burned and damaged personal digital devices, such as tablet computers and cell phones. At present, the digital devices are being stored as evidence and forensically preserved by the FBI.

19. The personal digital devices recovered to date are as follows:

- a. Apple iPhone x, imei 357207094385051;
- b. Apple iPhone 6s, imei 353296070333999;
- c. Apple iPhone 7, 355826083719624;
- d. Apple iPhone x, imei 354841095552369;
- e. Apple iPhone 6, imei 354411064453690; and
- f. Apple iPad a1954, sn GG7XK3DFJMXJ.

20. Evidence recovery from the P/V CONCEPTION WRECKAGE and debris field is ongoing.

21. Based upon my training and experience, it is my opinion that the personal digital devices recovered from the P/V CONCEPTION WRECKAGE belong to either the crew or deceased passengers and crewmember of the vessel.

22. Given the nature of the fire aboard the P/V CONCEPTION, and the large number of passengers trapped below deck during the fire, it is my opinion that digital devices recovered from the P/V CONCEPTION WRECKAGE may contain digital images, digital videos, text messages, digital audio recordings, and/or other documentary evidence of the events during the fire, and the events that led to the fire. Similarly, if any of the recovered digital devices belong to crewmembers of the P/V CONCEPTION, it is also my opinion that these devices may contain evidence of the events that led to the fire and evidence of the crew's response to that fire.

D. Additional Information Regarding SEA LANDING and TRUTH AQUATICS

23. On September 5, 2019, USCG-CGIS Special Agent Chris Zajackowski telephonically interviewed C.C.D., who previously worked as a captain and in an administrative capacity for TRUTH AQUATICS, INC. Special Agent Zajackowski informed me that he learned the following from that interview:

a. C.C.D. worked for TRUTH AQUATICS, INC. for approximately 17 years, ending in 2015.

b. C.C.D. managed the sales department for SEA LANDING, which he indicated is affiliated with TRUTH AQUATICS, INC.

c. C.C.D. was also the master (also known as captain) for approximately one year, and the second captain for approximately one year, for TRUTH AQUATICS, INC. He worked aboard the P/V CONCEPTION approximately four times, and also worked aboard the P/V TRUTH.

d. Regarding roving patrols, C.C.D. indicated that there was no "formal" watchman while vessels were underway or at anchor. Instead, C.C.D. would set the anchor alarm to detect vessel movements and also wake up periodically to check the vessel (for example, look around the decks and common spaces).

e. Company documents and records are kept at the aforementioned place of business for TRUTH AQUATICS, INC., 301 West Cabrillo Boulevard, Santa Barbara, California.

24. Based on my discussions with local law enforcement personnel, SEA LANDING sells dive charter trips out of the same

place of business that TRUTH AQUATICS, INC., is connected to, namely 301 West Cabrillo Boulevard, Santa Barbara, California.

25. On September 6, 2019, I visited the website www.sealanding.net. On that website, I discovered that a person could book island and diving excursions with vessels operated by TRUTH AQUATICS, INC., on the www.sealanding.net website.

26. On September 6, 2019, I conducted a "business search" on the California Secretary of State website. I searched using the name "Truth Aquatics," and the website indicated that the "entity address" is 301 West Cabrillo Boulevard, Santa Barbara, California.

E. The P/V TRUTH and P/V VISION

27. I have reviewed the current COI for the P/V TRUTH. The COI indicates that the vessel is owned by the same entity as the P/V CONCEPTION. It is also operated by TRUTH AQUATICS, INC., the same entity that operated the P/V CONCEPTION before it burned and sank. As with the P/V CONCEPTION, the P/V TRUTH's COI also requires that a member of the crew be designated as a "roving patrol" when passenger bunks are occupied.

28. I have reviewed the current COI for the P/V VISION. The COI indicates that the vessel is owned by "Glen Richard Fritzler Trustee," and the owner's address is listed as the address for TRUTH AQUATICS, INC. "Glen Richard Fritzler Trustee" is listed as the owner of the P/V CONCEPTION on at least one of that vessel's prior COI's. As with the P/V CONCEPTION, the P/V VISION's COI also requires a "designated

patrolman" when "passengers are in staterooms located below the main deck."

29. Based upon my review of the vessel COI's, photographs, and videos of the exteriors and interiors of the ship posted on TRUTH AQUATIC, INC.'s website, it is my understanding and opinion that the P/V VISION is similar in design, layout, build, and age to the P/V CONCEPTION.

30. The P/V TRUTH is slightly older and smaller than the P/V CONCEPTION, however it is used for the same purpose (diving and sightseeing trips), is operated by the same company as the P/V CONCEPTION, has a similar hull-type as the P/V CONCEPTION, and also has staterooms (berths) below the main deck.

31. I have reviewed a letter dated January 8, 1985, from the USCG to Glen Fritzler at TRUTH AQUATICS, INC. The letter is regarding electrical plans and installation for the P/V VISION. The letter notes that "[s]ince the electrical installation on the PROJECT X will be identical to the electrical installation on your present vessel M/V CONCEPTION (M/V ad P/V are interchangeable), your request to use the M/V CONCEPTION's approved electrical plans in lieu of submitting new electrical plans is approved." As such, it appears that the P/V VISION's electrical system is relevant to a review of the electrical system onboard the P/V CONCEPTION.

32. Based on my training and experience inspecting and operating vessels, as well as discussions with USCG personnel and other agents, I am informed and believe that ships owned and/or operated by the same company often contain similar

documentation, methods of operation, and posted notices. As such, given that the P/V VISION, P/V TRUTH, and P/V CONCEPTION are all operated by TRUTH AQUATICS, INC., the P/V VISION and P/V TRUTH will likely contain evidence relevant to the evaluation of the design, operation, and/or maintenance of the P/V CONCEPTION. In addition, the P/V VISION and P/V TRUTH may have information relevant to the origin and cause of the fire aboard the P/V CONCEPTION.

33. For example, based on the aforementioned, I anticipate that the following types of evidence relevant to the fire origin and cause determination for the P/V CONCEPTION, the determination of whether the P/V CONCEPTION crew posted a watchman or roving patrol, the determination of whether or not TRUTH AQUATICS, INC. experienced similar dive ship vessel fires in the past, and the determination as to why the 34 individuals were unable to escape from the below-deck bunk area on the P/V CONCEPTION, will be located aboard the P/V VISION and P/V TRUTH:

- a. Evidence of defective and/or non-compliant electrical equipment, systems, and/or components.
- b. Evidence of defective or non-compliant fire detection or suppression systems.
- c. Evidence of defective and/or non-compliant passenger safety and/or evacuation structures, systems, and/or procedures.
- d. Records and policies regarding compliance and/or non-compliance with federal, state, and/or local laws and/or regulations.

e. Records and logs reflecting the posting of a watchman, patrol, and/or roving patrol aboard vessels operated by TRUTH AQUATICS, INC.

f. Copies of local, state, and/or federal regulations and/or laws applicable to the operation of commercial dive and/or passenger vessels.

g. Records and logs of crewmember fire suppression and/or passenger safety drills or tests.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

34. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been

used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

35. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data

during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

36. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

//

//

//

//

//

VII. CONCLUSION

37. For all the reasons described above, I submit there is probable cause to believe that the items listed in Attachments B-1, B-2, B-3, and B-4, which constitute evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1115 (seaman's manslaughter) will be found at the premises as described in Attachments A-1, A-2, A-3, and A-4.

Jaime E. Wray
Special Agent
Coast Guard Investigative
Service

Subscribed to and sworn before me
this 7th day of September, 2019.

HONORABLE LOUISE A. LaMOTHE
UNITED STATES MAGISTRATE JUDGE

Magistrate Case Initiating Documents

[2:19-mj-03738 USA v. Search Warrant](#)

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

Notice of Electronic Filing

The following transaction was entered by Johns, Joseph on 9/7/2019 at 3:41 PM PDT and filed on 9/7/2019

Case Name: USA v. Search Warrant

Case Number: [2:19-mj-03738](#)

Filer: USA

Document Number: [1](#)

Docket Text:

APPLICATION for Search Warrant filed by Plaintiff USA. (Not for Public View pursuant to the E-Government Act of 2002) (Attachments: # (1) Proposed Warrant) (Attorney Joseph O Johns added to party USA(pty:pla)) (Johns, Joseph)

2:19-mj-03738-1 Notice has been electronically mailed to:

2:19-mj-03738-1 Notice has been delivered by First Class U. S. Mail or by other means BY THE FILER to :

The following document(s) are associated with this transaction:

Document description:Main Document

Original filename:C:\Users\nluqueno\Desktop\prem 4\Cover for SW Application_PremisesA4_PV Conception Wreckage MAW final.pdf

Electronic document Stamp:

[STAMP cacdStamp_ID=1020290914 [Date=9/7/2019] [FileNumber=28363591-0]
[5a30d27072bd5ee25fbbef8cd4b65283d8165147164c0d74037cef5f18c277d26056
05fac8ec10c6271c611079116f5a4fb5c9bd8b9c0739fc749d5e8b3d10a6]]

Document description:Proposed Warrant

Original filename:C:\Users\nluqueno\Desktop\prem 4\Cover for SW_PremisesA4_PV Conception Wreckage_SEALED MAW.pdf

Electronic document Stamp:

[STAMP cacdStamp_ID=1020290914 [Date=9/7/2019] [FileNumber=28363591-1]
[62e751117d87c6c5807ccee52d4ed4faaac873e2b75d8ac814a124f76c47f2848162
72fdc85ddb599bc7a519cecf5f188e7ee4438b5c76b61fcd7a8484ef304]]

BOYLAN 00061085

ATTACHMENT A-4

THE SUBJECT PREMISES

SUBJECT PREMISES A-4 is the vessel P/V CONCEPTION, Official Number 638133, including all remains of the wreckage, hull, and/or structures, and all debris and/or materials associated with the P/V CONCEPTION, including any digital devices recovered from the P/V CONCEPTION's wreckage and/or debris field (collectively, the "P/V CONCEPTION WRECKAGE"). The name "Conception" and the Official Number 638133 are painted on the side of the hull.

ATTACHMENT B-4

I. ITEMS TO BE SEIZED

The following is a list of items to be seized from SUBJECT PREMISES A-4, namely, the P/V CONCEPTION WRECKAGE, which constitute evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1115 (Seaman's Manslaughter):

1. The Passenger Vessel ("P/V") CONCEPTION, including all remains of the wreckage, hull, and/or structures, and all debris and/or materials associated with the P/V CONCEPTION, including any digital devices recovered from the P/V CONCEPTION's wreckage and/or debris field.

2. Evidence relating to the origin of the fire aboard the P/V CONCEPTION on or about September 2, 2019.

3. Evidence relating to the causation of the fire aboard the P/V CONCEPTION on or about September 2, 2019.

4. Evidence of custom, defective, and/or non-compliant electrical equipment, systems, and/or components on the P/V CONCEPTION.

5. Evidence of custom, defective, or non-compliant fire detection or suppression systems on the P/V CONCEPTION.

6. Evidence of custom, defective, and/or non-compliant passenger safety and/or evacuation structures, systems, and/or procedures on the P/V CONCEPTION.

7. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

8. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

g. applications, utility programs, compilers, interpreters, or other software, as well as documentation and

manuals, that may be necessary to access the device or to conduct a forensic examination of it;

h. records of or information about Internet Protocol addresses used by the device;

i. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

9. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

10. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to

store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

11. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

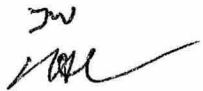
a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and

attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques~~[, including to search for known images of child pornography]~~. 

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

12. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.

Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

13. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

- a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;
- b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;
- c. Any magnetic, electronic, or optical storage device capable of storing digital data;
- d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;
- e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;
- f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and
- g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

14. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

EXHIBIT D

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

CONSENT TO SEARCH

1. I have been asked by Special Agents of the Federal Bureau of Investigation to permit a complete search of: (Describe the person(s), place(s), or thing(s) to be searched.)

- (1) Pink Apple iPhone, [REDACTED] found with [REDACTED] on or about 9/2/2019

2. I have been advised of my right to refuse consent.

3. I give this permission voluntarily.

4. I authorize these agents to take any items, which they determine may be related to their investigation.

2/19/2021
Date

[REDACTED]
Signature

Witness

[Signature]

EXHIBIT E

UNCLASSIFIED



Federal Bureau of Investigation
Digital Evidence Laboratory

ERF Building 27958A
Quantico, VA 22135

REPORT OF EXAMINATION

To: Los Angeles
Special Agent (SA) Joseph P. Hamer

Date: April 29, 2022
Case ID: 045-LA-3161932
Request No.: HQQ191205005

Request Date: September 13, 2019

Ref. No: Serial 409

Title: CONCEPTION DIVE BOAT,
TRUTH AQUATICS;
CRIMES ON THE HIGH SEAS

Date item(s) received: December 5, 2019

Item(s) submitted:

HQQ021384: Evidence Container, One Bag contains severely burned iPad parts (00192196)
(Not Examined)

HQQ022878: SIM Card, Sprint SIM Card model 63.09a ICCID: 8901120100 0644329136
(Not Examined)

HQQ021385: Evidence Container, One Bag contains severely burned cellphone parts
(00192191) (Not Examined)

HQQ022879: SIM Card, SIM Card ICCID: 89148 00000 44526 07115 (Not Examined)

HQQ021386: Cellular Phone, One Bag contains severely burned iPhone parts; (00192192)
(Examined)

HQQ022880: SIM Card, AT&T SIM Card (Not Examined)

HQQ021387: Evidence Container, One Bag contains severely burned cellphone parts

Page 1 of 3

An Accredited Laboratory
Since January 16, 2007



UNCLASSIFIED

UNCLASSIFIED

(00192190) (Not Examined)

HQQ021388: Evidence Container, One Bag contains severely burned cellphone parts (00192193) (Not Examined)

HQQ022881: SIM Card, Verizon SIM Card ICCID: 89148 00000 29431 94214 (Not Examined)

HQQ021389: Evidence Container, One Bag contains severely burned cellphone parts (00192194) (Not Examined)

HQQ022882: SIM Card, T-Mobile SIM Card (Not Examined)

HQQ021390: Evidence Container, One Bag contains severely burned cellphone parts (00192195) (Not Examined)

HQQ022883: SIM Card, Sprint SIM Card model 80.02a ICCID: 8901120200 0240084688 (Not Examined)

HQQ021391: Evidence Container, One Bag contains severely burned cellphone parts (00192188) (Not Examined)

Summary:

Per Electronic Communication dated December 16, 2019, SA Dennis Vollrath requested that the Electronic Device Analysis Unit (EDAU) examine the submitted evidence items associated with the captioned case. On April 8, 2022, the examination was transferred to the Computer Analysis Response Team (CART).

Evidence item HQQ021386 was severely damaged by water and fire, and required repairs three separate times by EDAU. After the third repair, a brute force attack was initiated to recover the device Personal Identification Number (PIN). The device PIN was successfully recovered, and an extraction was obtained from the device. The extraction was parsed, and its contents were exported to electronic reports. The extraction and examination results from HQQ021386 were copied to results media. None of the other evidence items submitted under this lab number were examined by CART.

Details of Examination:

The dates of this examination were April 15, 2021 through April 18, 2022.

Evidence item HQQ021386 was inventoried, labeled, and photographed.

Repairs were made to evidence item HQQ021386 by EDAU three separate times before CART could examine the device. After receiving evidence item HQQ021386 following the third repair, the device was connected to a forensic utility, and a brute force attack was initiated to recover the device PIN. The brute force completed successfully, and identified the device PIN as [REDACTED].

HQQ191205005
045-LA-3161932

UNCLASSIFIED

Evidence item HQQ021386 was unlocked using the recovered PIN, and was connected to another forensic utility. A logical extraction was obtained from HQQ021386. The extraction was parsed, and the contents of HQQ021386 were exported to electronic reports.

The extraction of HQQ021386 was copied to a Master Copy Blu-ray disc labeled HQQ027622. The examination results from HQQ021386 were copied to a Results Copy Blu-ray disc labeled HQQ027623.

None of the other evidence items submitted under this lab number were examined by CART.

Derivative Evidence/Copies:

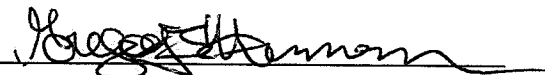
HQQ027622: Blu-ray Disc, One Blu-ray disc containing an archive copy of the extraction of HQQ021386; (MASTER COPY)

HQQ027623: Blu-ray Disc, One Blu-ray disc containing examination results from HQQ021386; (RESULTS COPY)

Disposition of Items:

Original evidence item HQQ021386, and derivative evidence items HQQ027622 and HQQ027623, were submitted to Operational Technology Division (OTD) evidence control for shipment to the contributor. The notes of examination are being placed in the OTD electronic case file. No electronic evidence is being retained by CART headquarters.

Examiner:


Gregory T. Hermanson
Operational Technology Division
Computer Analysis Response Team

HQQ191205005
045-LA-3161932

EXHIBIT F



Federal Bureau of Investigation
Digital Forensics Analysis Section

Operational Technology
ERF Building 27958A
Quantico, Virginia 22135

TECHNICAL ASSISTANCE REPORT

To: Los Angeles
Attn: SA Joseph P. Hamer/CART Dennis
Carl Vollrath

Date: April 20, 2022

Case ID: 45-LA-3161932
268-HQ-1305912-EE

Lab No.: HQQ191205005

Reference: Service Request dated December 16, 2019

Ref. No.: Serial 409

Title: Conception Dive Boat,
Truth Aquatics;
Crimes on the High Seas

Date specimen received: December 05, 2019

Specimens:

- HQQ021384 Apple iPad with 1B of 1B119 and San Diego (SD) RCFL of 00185086.
- HQQ021385 Apple iPad with an International Mobile Equipment Identity (IMEI) of 357207094385051, 1B of 1B134, and SDR CFL of 00185081.
- HQQ021386 Apple iPhone with 1B of 1B136 and SDR CFL of 00185082.
- HQQ021387 Apple iPhone with 1B of 1B117 and SDR CFL of 00185080.
- HQQ021388 Apple iPhone with an IMEI of 355826083719624, 1B of 1B135, and SDR CFL of 00185084.
- HQQ021389 Apple iPhone with 1B of 1B137 and SDR CFL of 00185085.
- HQQ021390 Apple iPhone with an IMEI of 354841095552369, 1B of 1B129, and SDR CFL of 00185083.

HQQ021391 Unknown Fragment of PCB with 1B of 1B118 and SDR CFL of 00185089.

HQQ022878 Sprint 63.09a Subscriber Identity Module (SIM) Card with an Integrated Circuit Card Identifier (ICCID) of 8901120100 0644329136.

HQQ022879 SIM Card with an ICCID of 89148 00000 44526 07115.

HQQ022880 SIM Card.

HQQ022881 Verizon SIM Card with an ICCID of 89148 00000 29431 94214.

HQQ022882 T-Mobile SIM Card.

HQQ022883 Sprint 80.02a SIM Card with an ICCID of 8901120200 0240084688.

Derivative Evidence (DE):

NONE

Summary:

The Electronic Device Analysis Unit (EDAU) was requested to process the submitted evidence.

Details:

All submitted evidence items were labeled and photographed. Additionally, the following procedures were performed.

The HQQ021384, HQQ021385, HQQ021388, HQQ021389, HQQ021390, and HQQ021391 specimens were each triaged by Supervisory Electronics Engineer (SEE) Michael McFarlane and determined to be significantly damaged with a possibility of data recovery. Initial attempts to repair were unsuccessful. At the request of Special Agent Joseph Hamer, further repair attempts are being halted at this time.

The HQQ021387 specimen was triaged by SEE McFarlane and determined to be damaged beyond repair.

No examination was performed by EDAU on the HQQ022878, HQQ022879, HQQ022881, HQQ022882, and HQQ022883 specimens.

The HQQ021386 and HQQ022880 specimens were transferred to CART for examination/extraction.

At the request of the field, all submitted evidence in EDAU's custody is being returned to the Los Angeles field office via Operational Technology Division (OTD) Evidence Control. At this time, EDAU considers this examination complete. The case notes and other supporting documents are being retained within the OTD case file.

Name:



Todd Prosser

Name:



Michael McFarlane

Operational Technology Division
Electronic Device Analysis Unit

EXHIBIT G

FBI Number	Description	ID Number	Date Seized	Location Seized	Successful extraction?	Basis for Search	Search Method
1B116	(U) Item 33 - Possible electronic device, Android		9/6/2019	Santa Barbara Harbor	No		Item 1B116 was fused into one piece and could not be prepared for further examination
1B117	(U) Item 32 - One (1) cellphone; Apple iPhone	HQQ021387	9/6/2019	Santa Barbara Harbor	No		4/20/22 - Triaged by SEE McFarlaneM and determined to be damaged beyond repair
1B118	(U) Item 31 - Portable electronic; Unknown Fragment of PCB	HQQ021391	9/6/2019	Santa Barbara Harbor	No		4/20/22 - Triaged by SEE McFarlaneM and determined to be significantly damaged with a possibility of data recovery. Initial attempts to repair were unsuccessful
1B119	(U) Item 30 - Tablet with black case; Apple iPad	HQQ021384	9/6/2019	Santa Barbara Harbor	No		4/20/22 - Triaged by SEE McFarlaneM and determined to be significantly damaged with a possibility of data recovery. Initial attempts to repair were unsuccessful
1B Digital	Sprint 63.09a SIM Card (ICCID: 8901120100 0644329136) (Found in same evidence bag as 1B119)	HQQ022878	9/6/2019	Santa Barbara Harbor	No		Not examined
1B127	(U) Item 22 - Hero 4 GoPro with case		9/5/2019	Santa Barbara Harbor	No		Not examined
1B129	(U) Item 20 - One (1) cellphone with case; Apple iPhone	HQQ021390	9/4/2019	Santa Barbara Harbor	No		4/20/22 - Triaged by SEE McFarlaneM and determined to be significantly damaged with a possibility of data recovery. Initial attempts to repair were unsuccessful
1B Digital	Sprint 80.02a SIM Card (ICCID: 8901120200 0240084688) (Found in same evidence bag as 1B129)	HQQ022883	9/4/2019	Santa Barbara Harbor	No		Not examined
1B134	(U) Item 15 - One (1) cellphone, Apple iphone with case and pop socket (Apple iPad?)	HQQ021385	9/4/2019	Santa Barbara County Coroner	No		4/20/22 - Triaged by SEE McFarlaneM and determined to be significantly damaged with a possibility of data recovery. Initial attempts to repair were unsuccessful
1B Digital	SIM Card (ICCID: 89148 00000 44526 07115) (Found in same evidence bag as 1B134)	HQQ022879	9/4/2019	Santa Barbara County Coroner	No		Not examined
1B135	(U) Item 14 - One (1) cellphone, Apple iphone with case	HQQ021388	9/4/2019	Santa Barbara County Coroner	No		4/20/22 - Triaged by SEE McFarlaneM and determined to be significantly damaged with a possibility of data recovery. Initial attempts to repair were unsuccessful
1B Digital	Verizon SIM Card (ICCID: 89148 00000 29431 94214) (Found in same evidence bag as 1B135)	HQQ022881	9/4/2019	Santa Barbara County Coroner	No		Not examined
1B136	(U) Item 13 - One (1) cellphone, pink Apple iphone	HQQ021386	9/4/2019	Santa Barbara County Coroner	Yes	Consent	8/11/22 - Cellebrite Extraction by SA HamerJ
1B Digital	SIM Card (Found in same evidence bag as 1B136)	HQQ022880	9/4/2019	Santa Barbara County Coroner	No		Not examined
1B137	(U) Item 12 - One (1) cellphone, silver Apple iphone	HQQ021389	9/4/2019	Santa Barbara County Coroner	No		4/20/22 - Triaged by SEE McFarlaneM and determined to be significantly damaged with a possibility of data recovery. Initial attempts to repair were unsuccessful
1B Digital	T-Mobile SIM Card (Found in same evidence bag as 1B137)	HQQ022882	9/4/2019	Santa Barbara County Coroner	No		Not examined
1B174	(U) Item 50 - One (1) cell phone with red case; Apple iPhone 7	HQQ018285	9/10/2019	Port Hueneme Exam Site	Yes	Search Warrant	9/27/2019 - Examination and extraction by SSA CooneyB; File System Extraction using GrayKey 1.11.11 (Device repaired by OssmanM)
1B175	(U) Item 49 - One (1) cell phone; Apple iPhone X	HQQ018280	9/10/2019	Port Hueneme Exam Site	No		4/5/22 - Evaluated by OssmanM and determined to be significantly damaged. Attempts to repair specimen were unsuccessful

	AT&T Sim Card (See 1B175) (ICCID: 89014104270511387531)	HQQ018281	9/10/2019	Port Hueneme Exam Site	No		Not examined
1B176	(U) Item 48 - One (1) camera	HQQ018282	9/10/2019	Port Hueneme Exam Site	No		Not examined
	SD Card; Damaged Secure Digital (SD) Card (Removed from 1B176)	HQQ018283	9/10/2019	Port Hueneme Exam Site	No		Evaluated by OssmanM and determined that no data was able to be extracted due to extensive physical damage
1B177	(U) Item 47 - One (1) ipad with reddish case; Apple iPad 4	HQQ018284	9/10/2019	Port Hueneme Exam Site	Yes	Search Warrant	9/23/2019 - Examination and extraction by SSA CooneyB; File System Extraction using GrayKey 1.11.11 (Device repaired by OssmanM)
1B227	(U) Possible electronic device		9/5/2019	Santa Barbara Harbor	No		Not examined
1B247	Samsung Galaxy S10	HQQ020454	9/11/2019	Port Hueneme Exam Site	No		8/22/22 - Evaluated by SEE McFarlaneM and determined to be significantly damaged with a possibility of data recovery
1B248	Samsung Galaxy S10	HQQ020457	9/11/2019	Port Hueneme Exam Site	No		8/22/22 - Evaluated by SEE McFarlaneM and determined to be significantly damaged with a possibility of data recovery
1B288	(U) Camera with Sim Card	HQQ020462	9/19/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to be damaged to an extent where data recovery was unlikely
1B289	(U) Item 303: Apple Tablet with Stylus	HQQ020462	9/20/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to be damaged to an extent where data recovery was unlikely
1B290	(U) Item 304: Portable Electronic Device; Apple A1662 iPhone SE	HQQ031144	9/20/2019	Port Hueneme Exam Site	Yes	Search Warrant	10/16/22 - Cellebrite Extraction Report by DFE Beltrank and SA HamerJ
1B290	SIM Card (ICCID: 89014102271386495336007646)	HQQ030328	9/20/2019	Port Hueneme Exam Site	No		Not examined
1B291	(U) Item 305: Camera	HQQ020462	9/20/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to be damaged to an extent where data recovery was unlikely
1B292	(U) Item 306: Pieces of Possible Electronic Device	HQQ020462	9/20/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to be damaged to an extent where data recovery was unlikely
1B293	(U) Item 327: Apple Digital Watch	HQQ020459	9/22/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to either contain no memory components which could contain data, or to be damaged to an extent where no data recovery was possible
1B294	(U) Item 329: iPhone	HQQ020452	9/22/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to either contain no memory components which could contain data, or to be damaged to an extent where no data recovery was possible
1B295	(U) Item 335: Camera	HQQ020448	9/22/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to either contain no memory components which could contain data, or to be damaged to an extent where no data recovery was possible
1B296	(U) Item 351: Cell Phone	HQQ020461	9/22/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to either contain no memory components which could contain data, or to be damaged to an extent where no data recovery was possible

1B297	(U) Item 352: Cell Phone	HQQ020455	9/22/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to either contain no memory components which could contain data, or to be damaged to an extent where no data recovery was possible
1B298	(U) Item 355: Electronic Device	HQQ020462	9/24/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to be damaged to an extent where data recovery was unlikely
1B299	(U) Item 356: Electronic Device		9/24/2019	Port Hueneme Exam Site	No		Not examined
1B300	(U) Item 358: Camera	HQQ020449	9/24/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to either contain no memory components which could contain data, or to be damaged to an extent where no data recovery was possible
1B301	(U) Item 359: Camera	HQQ020453	9/24/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to either contain no memory components which could contain data, or to be damaged to an extent where no data recovery was possible
1B302	(U) Item 360: Camera	HQQ020447	9/24/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to either contain no memory components which could contain data, or to be damaged to an extent where no data recovery was possible
1B303	(U) Item 361: Electronic	HQQ020456	9/24/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to either contain no memory components which could contain data, or to be damaged to an extent where no data recovery was possible
1B304	(U) Item 362: Electronic	HQQ020458	9/24/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to either contain no memory components which could contain data, or to be damaged to an extent where no data recovery was possible
1B305	(U) Item 363: Cell Phone Charred	HQQ020460	9/24/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to either contain no memory components which could contain data, or to be damaged to an extent where no data recovery was possible
1B306	(U) Item 366: Cell Phone	HQQ020450	9/24/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to either contain no memory components which could contain data, or to be damaged to an extent where no data recovery was possible
1B307	(U) Item 368: Phone	HQQ020451	9/24/2019	Port Hueneme Exam Site	No		8/22/22 - Triaged by SEE McFarlaneM and determined to either contain no memory components which could contain data, or to be damaged to an extent where no data recovery was possible
1B518	(U) Charred black and white mobile phone		10/15/2020	Santa Barbara Sheriff's Office	No		Damaged beyond the point of repair (See BOYLAN_00331310)
1B519	(U) Charred Silver iPhone	HQQ031638	10/15/2020	Santa Barbara Sheriff's Office	No	Consent	9/2/2022 - Evaluated by A. Wesley Chappell and determined to be significantly damaged with minimal chance of data recovery